IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant:	FRANK T. WICZKOWSKI		
Serial No.:	10/085,351	Art Unit:	3692
Filed:	February 28, 2002	Examiner:	C. B. Graham
For:	METHOD OF CONDUCTING ANONYMOUS TRANSACTIONS OVER THE INTERNET		

Commissioner for Patents
Mail Stop AF
Box 1450
Alexandria, VA 22313-1450

S I R:

AFFIDAVIT UNDER 37 C.F.R. §1.131

I, Frank T. Wiczkowski, hereby declare that:

1. I am the sole applicant and owner of the above-captioned patent application, which has a filing date of February 28, 2002.

2. My patent attorney, Larry W. Miller, Reg. No. 29,417, who has the power of attorney in the above-captioned patent application, explained to me that all claims we have presented in this application have been rejected as being anticipated by U. S. Patent Publication No. 2001/0034725 (Park) which was published on October 25, 2001, from an application filed on March 14, 2001, which claims priority on a Korean national application filed on March 14, 2000.

3. Attached to this Affidavit is a copy of an entry in my planner, which is attached hereto as Exhibit A, that I made in August, 1999 (using a recycled planner from 1998) to

document the concept of an invention for a secure anonymous transaction process over the Internet through the use of a proxy server. My initial conception of this idea was made in the previous month (July, 1999) while working on a project to process credit card micro transactions over the Internet. Thus, I hereby declare that I conceived this invention prior to the March 14, 2000, filing date of the Park priority application.

4. This planner entry (Exhibit A) states "New service idea....ID theft & anonymous purchase" on the left side of the planner with an arrow pointing to a schematic that identifies a first box as a "Customer Credit Card Database" with a line connecting a second box identified as "Secure Database & Proxy Server" having another line connecting to a third box identified as "Our Purchasing ID Database & Our Credit Card DB". From the second box, another line connects a "cloud" that is labeled "Fire Wall" with an arrow pointing to the words "To Internet". This schematic is the basic concept of the secure anonymous transaction process.

5. In the latter half of 1999, I conducted research into the credit card industry and their electronic methods of operation. As part of this research, I also investigated credit card fraud on the Internet as well as the current systems in place to reduce such fraud. I found that identity theft via the Internet was growing exponentially. By the end of 1999, I was convinced that my idea of providing a secured anonymous transaction for internet sales would provide a good solution to both problems of credit card fraud and identity theft.

6. In the first quarter of 2000, I started to refine my general idea of a secured anonymous transaction by establishing the minimum hardware and software environments that would be required for up to 10,000 users, as is reflected in the block diagram attached hereto as Exhibit B. My research in 1999 had shown that the banking and credit card industries required a minimum of 10,000 users as proof of a concept solution. I was integrating this idea into my telecommunications company, MAW Communications, which is a Pennsylvania based competitive local exchange carrier.

7. During the first half of 2000, I attempted to obtain funding for the development of my invention. Primarily, I prepared an application for a Small Business Administration (SBA) loan for my company, MAW Communication, that included the submission of a platform specification that would support the operation of my secure anonymous transaction idea. To that end, I worked with Telcordia Technologies to develop from their standard hardware configurations an IP Rapid Deployment Platform. In June, 2000, I obtained from Telcordia Technologies a 13 page description of their IP Rapid Deployment Platform on which I would be able to base the continued development of my invention to provide a secured anonymous transaction process for the Internet. I cannot attached a copy of this document, as the document is deemed confidential and is not to be made publically available.

8. During the second half of 2000, the dot com meltdown took the telecommunications industry down with it. My company, MAW Communications, suffered financially also. As a result, development of my invention was slowed; however, I continued to work on details of the various components of the system, continued to seek funding for the development of the hardware and software necessary to place my invention into operation, and continued to conduct research into the identity theft issues and credit card transactions.

9. In 2001, I was able to re-establish the cash flow of my company; however, I knew that a substantial amount of capital would be necessary to fully develop the invention. Thus, I decided to make a presentation to Telcordia Technologies to seek their investment into my invention. By May, 2001, I had developed an extensive Powerpoint presentation and made a presentation to Telcordia Technologies. Also attached hereto is a page from the Powerpoint presentation to Telcordia Technologies, marked as Exhibit C.

10. In the fourth quarter of 2001, I completed the refinement of the details of the process so that the documentation could be used as a project development specification, as is represented in the flow diagram of Exhibit D.

11. I contacted a local patent attorney, Larry W. Miller, to prepare and file a patent application for my invention on January 30, 2002. Mr. Miller prepared the patent application and filed it on February 28, 2002.

12. I believe that the Exhibits B through D show diligence from the date of conception of my invention in July, 1999, until the filing of the patent application. Diligence is reflected in the seeking of funding to development the invention, research to better define the problems that were being encountered in the industry, and the development of details of the various steps. At no time during the period between July, 1999, and February 28, 2002, did I stop work on the invention for any significant period of time.

13. I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

Respectfully submitted,

Date: 9/10/07

Frank T. Wiczkowski

AUGUST 1998

SUNDAY	MONDAY	TUESDAY	WEDNESDAY
2	3	4	5
9	10	11	12
16	17	18	19
23	24	25	26
30	31		

July

S	M	T	W	T	F	S
			1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30	31	

AUGUST 1998

THURSDAY	FRIDAY	SATURDAY	TO BE DONE
6	7	8	
13	14	15	
20	21	22	NOTES AND MEMOS
27	28	29	

September

S	M	T	W	T	F	S
		1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30			

Exhibit "B"

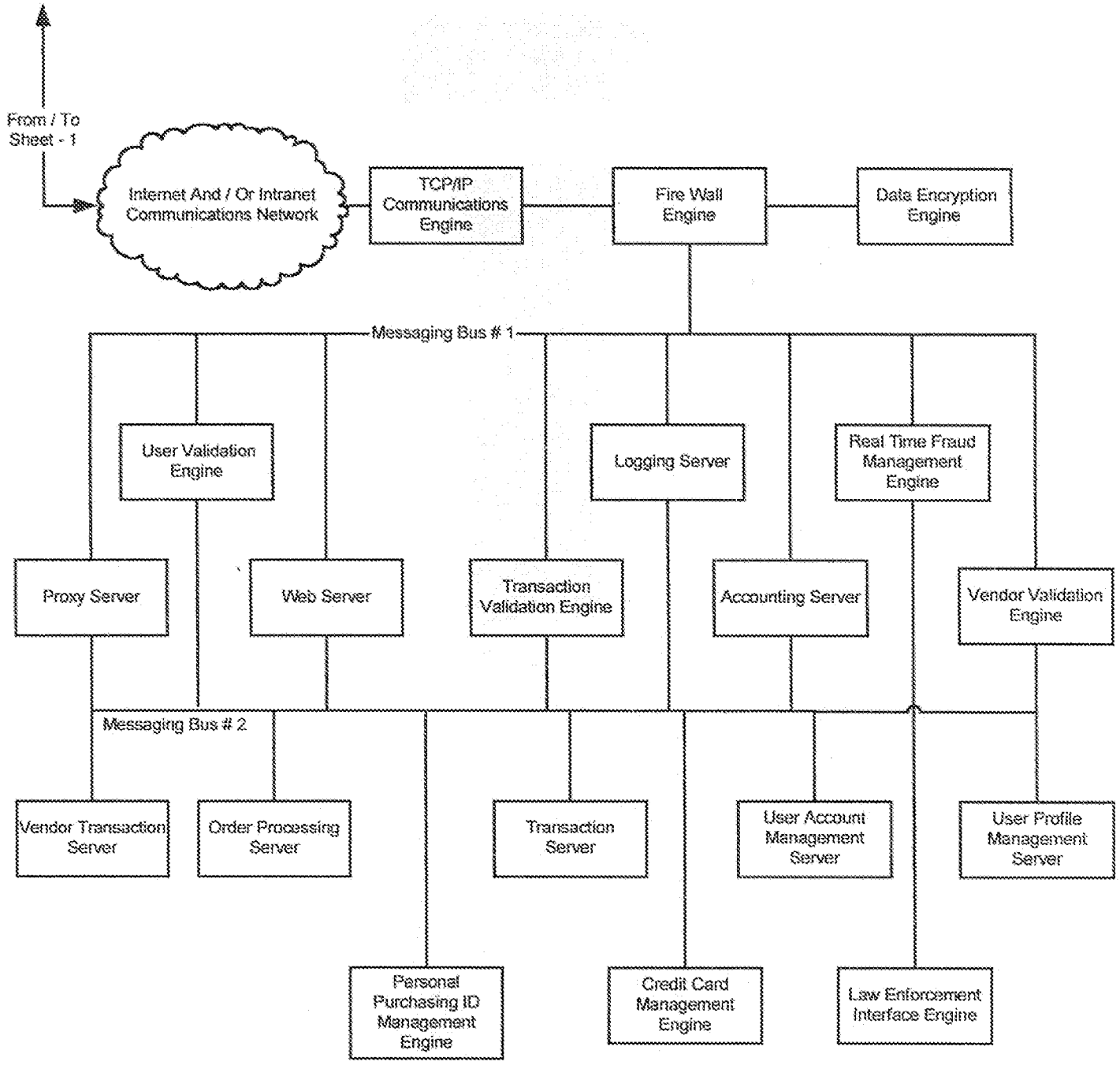

From / To
Sheet - 1
Internet And / Or Intranet
Communications Network
TCP/IP
Communications
Engine
Fire Wall
Engine
Data Encryption
Engine
Messaging Bus # 1
User Validation
Engine
Logging Server
Real Time Fraud
Management
Engine
Proxy Server
Web Server
Transaction
Validation Engine
Accounting Server
Vendor Validation
Engine
Messaging Bus # 2
Vendor Transaction
Server
Order Processing
Server
Transaction
Server
User Account
Management
Server
User Profile
Management
Server
Personal
Purchasing ID
Management
Engine
Credit Card
Management
Engine
Law Enforcement
Interface Engine

Exhibit "C"

The problem ….

- Most consumers do not feel the Internet is secure.
- Identity Fraud Risk (IFR) increases exponentially with the number of sites containing your personal information. Sites of all sizes are regularly hacked, with information theft as the main goal of the hack.
- Personal information is regularly used and sold to target market goods and services to the consumer.
- In its present form, most people are correct. The Internet is not secure.

The cause ….

- The net's current purchasing systems require the purchaser to provide confidential, personal information to complete a transaction.
- Anybody, with a little money, can act as a vendor, make credit card transactions, and control the consumer's personal information. The net operates without standardized controls or systems integrity testing requirements.
- The most current technology is always available to hackers and the rewards for a successful hack can be enormous.

The effect ….

- Consumer net spending is significantly limited due to the lack of consumer trust in the security of the net.
- B2C – E-Commerce growth is limited by the consumer's trust or willingness to share personal information on the net.
- Credit card fraud and identity fraud is big business and is a world wide problem.

The solution ….

- Create a system whereby a third party clearing house secures a consumer's personal information for all of the consumer's net purchasing.
- The clearing house performs the consumer's purchases via secure proxy.
- The clearing house utilizes a series of credit card numbers that are used for a limited number of transactions, and are assigned to the clearing house.

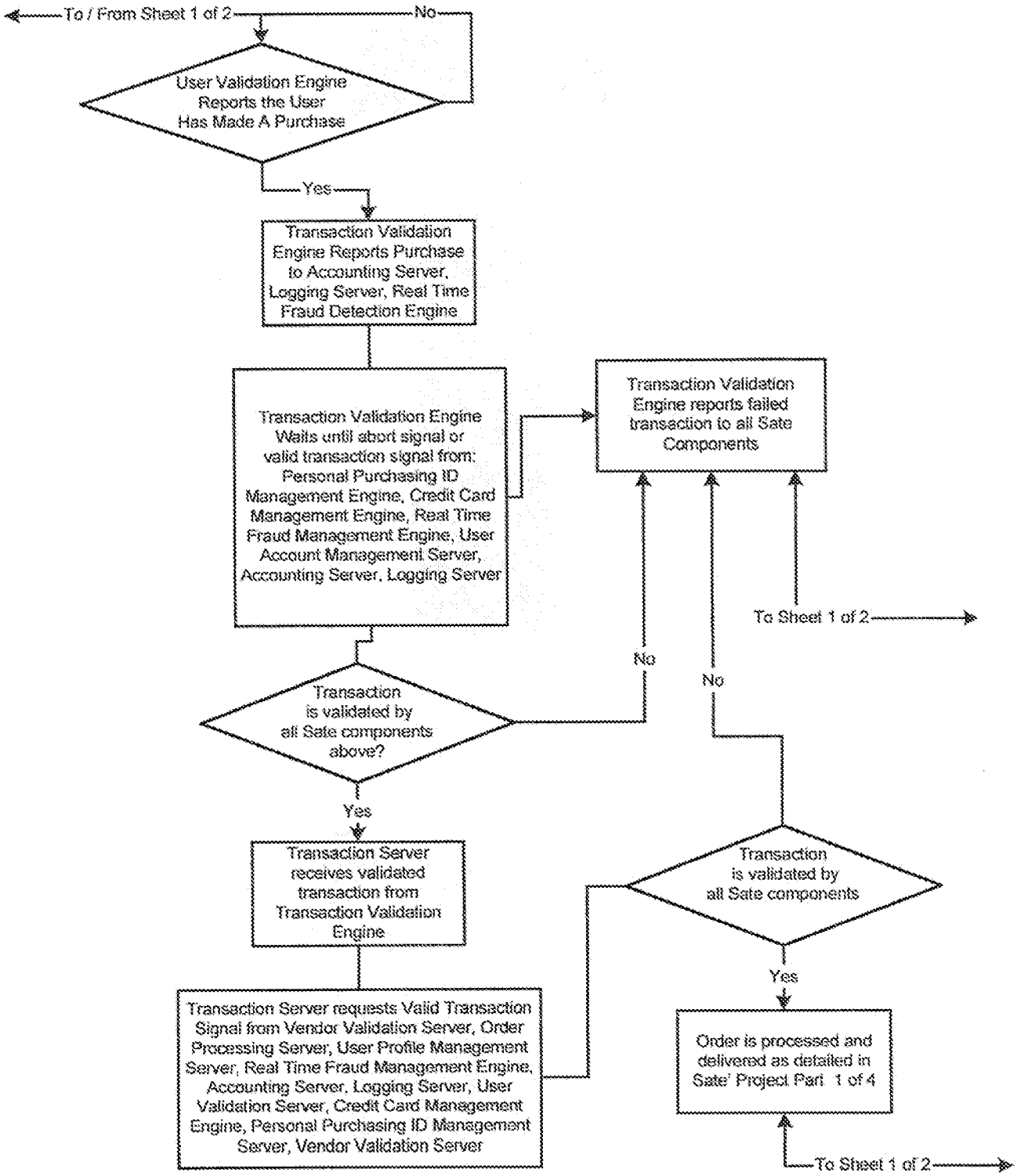
The results ….

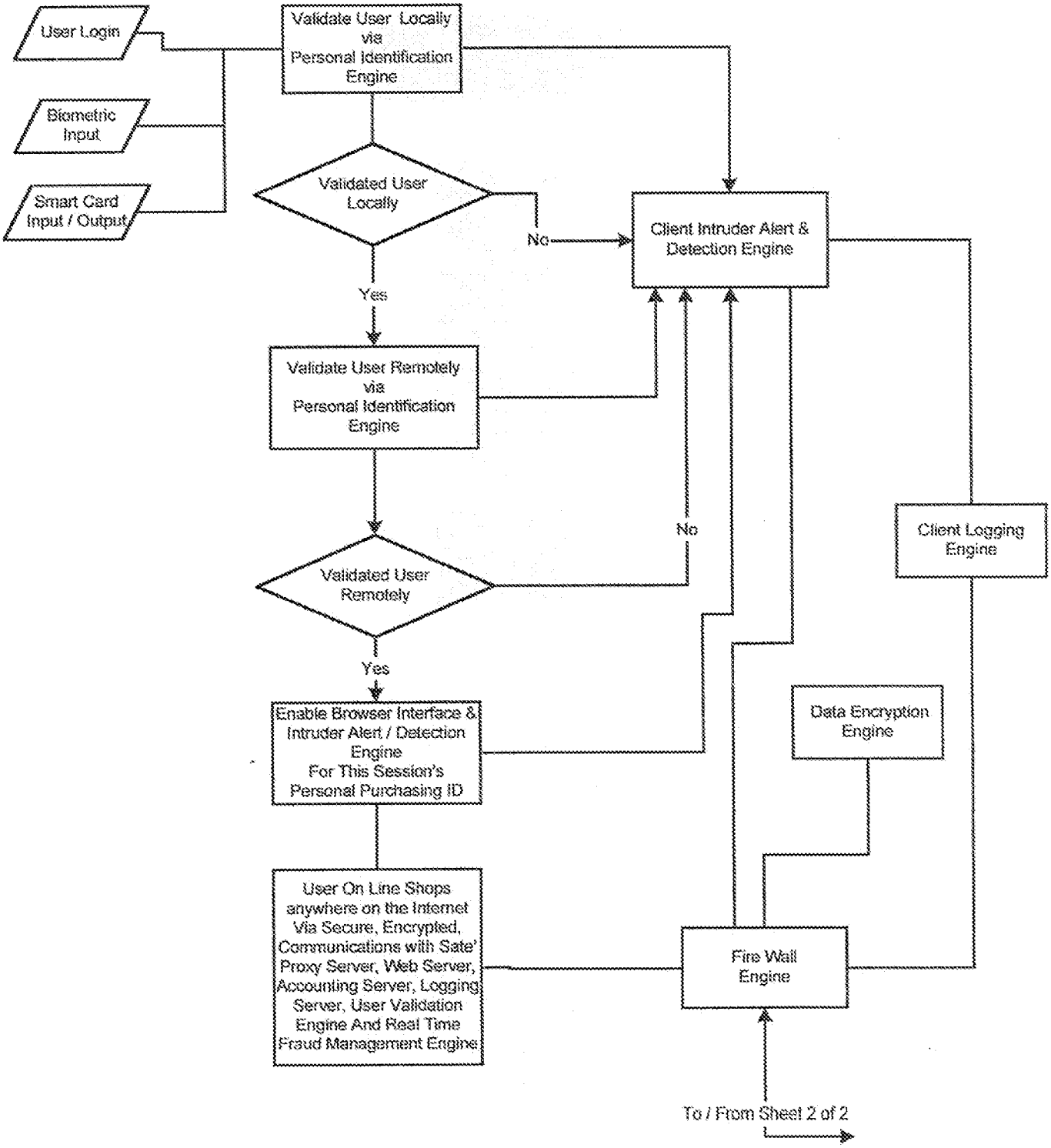
- The consumer's personal information remains personal. IFR is significantly reduced and does not grow with the consumer's activities on the net.
- Consumer willingness to purchase on the net is no longer inhibited by the increased risk of fraud and loss of privacy. In fact, privacy is enhanced. Purchasing can be accomplished anonymously, using a Personal Purchasing ID (PPID).
- Credit card fraud and identity fraud are significantly harder to accomplish.

How do we create the solution to get the results?

We create a Secure Anonymous Transaction Engine … Sate

Exhibit "D"


To / From Sheet 1 of 2
No
User Validation Engine Reports the User Has Made A Purchase
Yes
Transaction Validation Engine Reports Purchase to Accounting Server, Logging Server, Real Time Fraud Detection Engine
Transaction Validation Engine Waits until abort signal or valid transaction signal from: Personal Purchasing ID Management Engine, Credit Card Management Engine, Real Time Fraud Management Engine, User Account Management Server, Accounting Server, Logging Server
Transaction Validation Engine reports failed transaction to all Sate Components
To Sheet 1 of 2
No
Transaction is validated by all Sate components above?
No
Yes
Transaction Server receives validated transaction from Transaction Validation Engine
Transaction is validated by all Sate components
Yes
Transaction Server requests Valid Transaction Signal from Vendor Validation Server, Order Processing Server, User Profile Management Server, Real Time Fraud Management Engine, Accounting Server, Logging Server, User Validation Server, Credit Card Management Engine, Personal Purchasing ID Management Server, Vendor Validation Server
Order is processed and delivered as detailed in Sate' Project Part 1 of 4
To Sheet 1 of 2


User Login
Biometric Input
Smart Card Input / Output
Validate User Locally via Personal Identification Engine
Validated User Locally
No
Yes
Client Intruder Alert & Detection Engine
Validate User Remotely via Personal Identification Engine
No
Validated User Remotely
Yes
Client Logging Engine
Enable Browser Interface & Intruder Alert / Detection Engine For This Session's Personal Purchasing ID
Data Encryption Engine
User On Line Shops anywhere on the Internet Via Secure, Encrypted, Communications with Sate' Proxy Server, Web Server, Accounting Server, Logging Server, User Validation Engine And Real Time Fraud Management Engine
Fire Wall Engine
To / From Sheet 2 of 2